PCT/JP00/07682
01.11.00
09/869515

JP 00/7682

EKW

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 17 NOV 2000
WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１１月　５日

出願番号
Application Number: 平成１１年特許願第３１４５２１号

出願人
Applicant (s): ソニー株式会社

２０００年　９月　８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０７３０９１

【書類名】　特許願

【整理番号】　9900479603

【提出日】　平成11年11月 5日

【あて先】　特許庁長官殿

【国際特許分類】　H04L 9/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　赤池　正光

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100082131

【弁理士】

【氏名又は名称】　稲本　義雄

【電話番号】　03-3369-6479

【手数料の表示】

【予納台帳番号】　032089

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ処理装置およびデータ処理方法、並びに記録媒体

【特許請求の範囲】

【請求項１】　データとともに、そのデータの宛先が配置されたデータブロックを処理するデータ処理装置であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、前記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索手段と、

前記注目エントリに登録された前記エントリ有効情報に基づいて、前記注目エントリが有効かどうかを判定する判定手段と、

前記判定手段による判定結果に基づいて、前記データブロックに配置されたデータの出力を制御する出力制御手段と

を備えることを特徴とするデータ処理装置。

【請求項２】　前記出力制御手段は、

前記注目エントリが有効である場合に、前記データを、前記データブロックに配置された宛先に出力し、

前記注目エントリが有効でない場合に、前記データを破棄する

ことを特徴とする請求項１に記載のデータ処理装置。

【請求項３】　前記データは暗号化されており、

その暗号化されたデータを復号する復号手段をさらに備える

ことを特徴とする請求項１に記載のデータ処理装置。

【請求項４】　前記データは、そのデータの宛先に割り当てられた鍵を用いて暗号化されており、

前記テーブルの各エントリには、前記宛先およびエントリ有効情報の他、その宛先に割り当てられた鍵も登録されており、

前記復号手段は、前記テーブルに登録されている前記鍵を用いて、前記データを復号する

ことを特徴とする請求項３に記載のデータ処理装置。

【請求項５】　前記復号手段は、前記テーブルの、前記データブロックの宛先に割り当てられた前記鍵を用いて、そのデータブロックに配置されたデータを復号する

ことを特徴とする請求項４に記載のデータ処理装置。

【請求項６】　前記テーブルの各エントリには、前記宛先、エントリ有効情報、および鍵の他、その鍵が有効かどうかを表す鍵有効情報も登録されており、

前記復号手段は、

前記データブロックの宛先に割り当てられた前記鍵の鍵有効情報に基づいて、その鍵が有効かどうかを判定し、

有効である場合に、前記鍵を用いて、データを復号する

ことを特徴とする請求項５に記載のデータ処理装置。

【請求項７】　前記テーブルの各エントリには、前記宛先およびエントリ有効情報の他、その宛先に割り当てられた２以上の鍵が登録されている

ことを特徴とする請求項４に記載のデータ処理装置。

【請求項８】　前記テーブルの各エントリには、前記２以上鍵それぞれについて、その鍵が有効かどうかを表す鍵有効情報が登録されている

ことを特徴とする請求項７に記載のデータ処理装置。

【請求項９】　前記テーブルを記憶するテーブル記憶手段をさらに備える

ことを特徴とする請求項１に記載のデータ処理装置。

【請求項１０】　前記宛先は、前記データを受信すべき通信端末のＭＡＣ(Media Access Control)アドレスである

ことを特徴とする請求項１に記載のデータ処理装置。

【請求項１１】　前記データブロックは、ＤＶＢ(Digital Video Broadcasting)の規格に準拠したものである

ことを特徴とする請求項１に記載のデータ処理装置。

【請求項１２】　１チップのＩＣ(Integrated Circuit)で構成される

ことを特徴とする請求項１に記載のデータ処理装置。

【請求項１３】　データとともに、そのデータの宛先が配置されたデータブロックを処理するデータ処理方法であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、前記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、

前記注目エントリに登録された前記エントリ有効情報に基づいて、前記注目エントリが有効かどうかを判定する判定ステップと、

前記判定ステップによる判定結果に基づいて、前記データブロックに配置されたデータの出力を制御する出力制御ステップと

を備えることを特徴とするデータ処理方法。

【請求項１４】　データとともに、そのデータの宛先が配置されたデータブロックを、コンピュータに処理させるプログラムが記録されている記録媒体であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、前記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、

前記注目エントリに登録された前記エントリ有効情報に基づいて、前記注目エントリが有効かどうかを判定する判定ステップと、

前記判定ステップによる判定結果に基づいて、前記データブロックに配置されたデータの出力を制御する出力制御ステップと

を備えるプログラムが記録されている

ことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ処理装置およびデータ処理方法、並びに記録媒体に関し、特に、例えば、データを、衛星回線等によって同報する場合に、そのデータを取得することのできる端末（ユーザ）を、容易に制限することができるようにするデータ処理装置およびデータ処理方法、並びに記録媒体に関する。

【０００２】

【従来の技術】

例えば、画像や音声等をディジタルデータで伝送する場合には、アナログ信号で伝送する場合と同一の伝送帯域で複数チャンネルを確保したり、また、より高品質の画像や音声を提供することが可能であり、衛星放送あるいは衛星通信等の分野では、画像や音声をディジタルデータで提供するシステムの普及が進んでいる。例えば、国内ではSkyPerfecTV!やDirecTV、北米ではDirecTV、欧州ではCanal Plus、といったディジタル衛星放送サービスが、それぞれ開始されている。放送のディジタル化は、１チャンネル当たりの送信コストの低減や、コンピュータで扱われるプログラムやデータの提供等を可能とし、また、ディジタル化により、プログラム等と画像等とを連動して提供するようなサービスも普及しつつある。

【０００３】

ディジタル衛星放送サービスでは、画像や音声のディジタルデータが、ＭＰＥＧ(Moving Picutre Experts Group)２や、このＭＰＥＧ２から派生したＤＶＢ(Digital Video Broadcasting)の規格に準拠したフォーマットに変換され、さらに多重化されて、電波として送信される。電波は、衛星のトランスポンダで受信され、増幅その他の必要な処理が施された後、地上に向けて送出される。

【０００４】

トランスポンダの伝送帯域は、例えば、３０Ｍｂｐｓ(Mega bit per second)と大きく（但し、トランスポンダでは、一般に、エラー訂正符号が付加されるので、３０Ｍｂｐｓの伝送帯域を有していても、実質的な伝送帯域は、最大で２７Ｍｂｐｓ程度）、このような大きな伝送帯域の全部を利用することで、ディジタルデータを、高品位で、かつ高速に配信することが可能である。

【０００５】

しかしながら、一般には、主に、コスト上の理由から、トランスポンダの伝送帯域は、多チャンネルに分割されて使用されることが多い。この場合、各チャンネルで伝送されるディジタルデータの内容は異なっていても、各チャンネルのディジタルデータを受信する受信側の仕組みは共通であるため、あるディジタルデ

ータの提供を、特定のユーザだけが受けることができるような限定受信（ＣＡ(Conditional Access)）機構が必要となる。

【０００６】

即ち、特に、例えば、いわゆるデータ放送を行う場合には、画像や音声を配信する場合に比較して、１番組当たりのデータ量が小さく、課金単位あるいは課金形態が複雑になることが予想され、これに対処するには、より細かな受信制御を行うことができる限定受信機構が必要となる。また、限定受信機構は、機密情報を配信する場合にも、その漏洩を防止するために必要となる。

【０００７】

一般に、限定受信機構は、配信するデータストリームに対して暗号化を施すことによって実現される。暗号化方式としては、大きく分けて、共通鍵暗号化方式（秘密鍵暗号化方式）と、公開鍵暗号化方式とが知られている。ディジタル衛星放送では、暗号化／復号の処理の負荷が、公開鍵暗号化方式に比較して軽いことから、共通鍵暗号化方式が用いられることが多い。

【０００８】

共通鍵暗号化方式では、ある契約者Ａに対して、暗号鍵と同一の、復号鍵となる符号列を何らかの方法で渡し、データが、暗号鍵で暗号化されて配信される。暗号化されたデータは、それから、暗号鍵（復号鍵）や元のデータを逆計算する等して類推することが困難なようになっており、従って、契約者でないユーザＢは、暗号化されたデータを受信しても、それを、元のデータに正しく復元することはできない。また、契約者であるユーザＡは、暗号化されたデータを、契約することにより渡された復号鍵で復号することにより、元のデータを復元することができる。従って、受信契約とは、復号鍵の引き渡しを行うことと等価である。

【０００９】

【発明が解決しようとする課題】

ところで、例えば、いま、ユーザＡとＣが契約者である場合において、ユーザＡだけとの契約が終了したり、あるいは、ユーザＡが不正な行為をしたときには、いままで使用していた暗号鍵を変更し、その変更後の暗号鍵と同一の復号鍵を、ユーザＣのみに提供すれば、その後は、契約者でなくなった、あるいは不正な

行為を行ったユーザＡは、新たな暗号鍵で暗号化されたデータを復元することができなくなるとともに、正当な契約者であるユーザＣは、続けて、新たな暗号鍵で暗号化されたデータを、新たな復号鍵で復号することにより正常に復元することができる。

【００１０】

しかしながら、あるユーザの契約が終了したり、不正な行為を発見するごとに、暗号鍵を変更し、さらに、変更後の暗号鍵と同一の復号鍵を、正当な契約者に提供するのは面倒である。

【００１１】

本発明は、このような状況に鑑みてなされたものであり、データを正常に取得する（受信する）ことのできるユーザを、容易に制限することができるようにするものである。

【００１２】

【課題を解決するための手段】

本発明のデータ処理装置は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索手段と、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定手段と、判定手段による判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御手段とを備えることを特徴とする。

【００１３】

出力制御手段には、注目エントリが有効である場合に、データを、データブロックに配置された宛先に出力させ、注目エントリが有効でない場合に、データを破棄させることができる。

【００１４】

データが暗号化されている場合には、データ処理装置には、暗号化されたデータを復号する復号手段をさらに設けることができる。

【００１５】

データが、そのデータの宛先に割り当てられた鍵を用いて暗号化され、テーブルの各エントリに、宛先およびエントリ有効情報の他、その宛先に割り当てられた鍵も登録されている場合には、復号手段には、テーブルに登録されている鍵を用いて、データを復号させることができる。

【００１６】

復号手段には、テーブルの、データブロックの宛先に割り当てられた鍵を用いて、そのデータブロックに配置されたデータを復号させることができる。

【００１７】

テーブルの各エントリに、宛先、エントリ有効情報、および鍵の他、その鍵が有効かどうかを表す鍵有効情報も登録されている場合には、復号手段には、データブロックの宛先に割り当てられた鍵の鍵有効情報に基づいて、その鍵が有効かどうかを判定させ、有効であるときに、鍵を用いて、データを復号させることができる。

【００１８】

テーブルの各エントリには、宛先およびエントリ有効情報の他、その宛先に割り当てられた２以上の鍵も登録することができる。

【００１９】

テーブルの各エントリには、２以上鍵それぞれについて、その鍵が有効かどうかを表す鍵有効情報も登録することができる。

【００２０】

本発明のデータ処理装置には、テーブルを記憶するテーブル記憶手段をさらに設けることができる。

【００２１】

宛先は、データを受信すべき通信端末のＭＡＣ(Media Access Control)アドレスとすることができる。

【００２２】

データブロックは、ＤＶＢ(Digital Video Broadcasting)の規格に準拠したものとすることができる。

【００２３】

本発明のデータ処理装置は、１チップのＩＣ(Integrated Circuit)で構成することができる。

【００２４】

本発明のデータ処理方法は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定ステップと、判定ステップによる判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御ステップとを備えることを特徴とする。

【００２５】

本発明の記録媒体は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定ステップと、判定ステップによる判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御ステップとを備えるプログラムが記録されていることを特徴とする。

【００２６】

本発明のデータ処理装置およびデータ処理方法、並びに記録媒体においては、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照することで、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリが、注目エントリとして検索される。そして、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかが判定され、その判定結果に基づいて、データブロックに配置されたデータの出力が制御される。

【００２７】

【発明の実施の形態】

図１は、本発明を適用した放送システム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない）の一実施の形態の構成例を示している。

【００２８】

図１の実施の形態においては、放送システムは、送信システム１、衛星２、受信システム３、およびネットワーク４から構成されている。なお、図１では、図が煩雑になるのを避けるため、１の受信システム（受信システム３）しか図示していないが、受信システムは、２以上設けることが可能である。

【００２９】

送信システム１は、制御装置１１、データサーバ１２、送信処理装置１３、アンテナ１４、回線接続装置１５、およびケーブル１６で構成され、制御装置１１、データサーバ１２、送信処理装置１３、および回線接続装置１５は、ケーブル１６を介して相互に接続されることで、ＬＡＮ(Local Area Network)を構成している。

【００３０】

制御装置１１は、データサーバ１２を制御することにより、送信処理装置１３に対して、衛星放送で配信すべきデータを供給させる。また、制御装置１１は、回線接続装置１５を制御することにより、インターネット等の外部のネットワーク４から、衛星放送で配信すべきデータを取得させ、送信処理装置１３に対して供給させる。さらに、制御装置１１は、送信処理装置１３における各種の処理を制御する。

【００３１】

データサーバ１２は、衛星放送で配信すべきデータを記憶しており、制御装置１１の制御にしたがって、必要なデータを、送信処理装置１３に供給する。

【００３２】

送信処理装置１３は、制御装置１１の制御にしたがい、データサーバ１２や回線接続装置１５から供給されるデータを、例えば、ＩＰ(Internet Protocol)パケットにパケット化し、さらに、そのＩＰパケットを、ＤＶＢデータ放送仕様に

準拠したセクション、即ち、例えば、EN 301 192 V1.1.1(1997-12), DVB specification for data broadcasting ETSI(European Telecommunications Standards Institute)で規定されているマルチプロトコルエンキャプスレイション(Multiprotocol Encapsulation)に基づくディスクリプタで記述されたセクションと呼ばれるデータブロックにブロック化する。そして、送信処理装置１３は、セクションを、所定長のペイロードに分割し、各ペイロードに、ＭＰＥＧ２のトランスポートストリームを構成するパケット（以下、適宜、ＴＳ(Transport Stream)パケットという）のヘッダを付加することで、ＴＳパケットに類するパケットを構成し、さらに、変調、増幅等の必要な処理を施して、アンテナ１４から、衛星放送波として送出する。

【００３３】

また、送信処理装置１３は、受信システム３を構成する端末24_1，24_2，・・・（図１において図示していない受信システムを構成する端末についても同様）それぞれのＭＡＣアドレスと、各ＭＡＣ(Media Access Control)アドレスに割り当てた暗号鍵とを対応付けた表形式の暗号鍵テーブルを記憶している暗号鍵テーブル記憶部１３Ａを有している。なお、各ＭＡＣアドレスに割り当てる暗号鍵は、基本的には、すべて異なるものとする。但し、一部のＭＡＣアドレスについて、同一の暗号鍵を割り当てるようにしても良い。

【００３４】

ここで、ＭＡＣアドレスとは、ＩＥＥＥ(Institute of Electrical Electronics Engineers)８０２．３等に適用されるアドレス体系であり、通信ポートごとに固有の４８ビットの値で、重複がないことが保証されている。４８ビットのＭＡＣアドレスは、その上位２４ビットが、ＩＥＥＥによって登録／管理される製造者（ベンダ(vendor)）識別番号となっており、その下位２４ビットが、各ベンダによって管理される機器識別番号となっている。ＭＡＣアドレスによれば、受信システム３の各端末24_i（ｉ＝１，２，・・・）を特定することができる。

【００３５】

上述のマルチプロトコルエンキャプスレイションによれば、セクションのヘッダ（セクションヘッダ）には、そのセクションのペイロードに配置されたデータ

を配信する端末２４$_i$の宛先として、その端末のＭＡＣアドレスが配置されるようになっている。セクションのペイロードに配置されるデータ、即ち、ここでは、ＩＰパケットを暗号化する必要がある場合には、送信処理装置１３は、セクションのヘッダに配置される宛先としての、端末２４$_i$のＭＡＣアドレスに割り当てられた暗号鍵を、暗号鍵テーブル記憶部１３Ａに記憶された暗号鍵テーブルから読み出し、その暗号鍵で、そのセクションのペイロードに配置されるＩＰパケットを暗号化するようになっている。

【００３６】

なお、暗号鍵テーブルは、受信システム３を構成する、後述する受信装置２２が有する鍵テーブルと同一形式のものであっても良いし、異なる形式のものであっても良い。また、ここでは、暗号鍵テーブルを、送信システム１に内蔵させておくようにしたが、暗号鍵テーブルは、例えば、ネットワーク４上の図示せぬサーバに記憶させておき、必要に応じて、回線接続装置１５を介して読み出して使用するようにすることも可能である。

【００３７】

回線接続装置１５は、例えば、モデムや、ＴＡ(Terminal Adapter)およびＤＳＵ(Digital Service Unit)等で構成され、ネットワーク４を介しての通信制御を行うようになっている。

【００３８】

受信システム３は、アンテナ２１、受信装置２２、回線接続装置２３、端末２４$_1$，２４$_2$，・・・、およびケーブル２５で構成されており、受信装置２２、回線接続装置２３、端末２４$_1$，２４$_2$，・・・は、ケーブル２５を介して相互に接続され、これにより、例えば、イーサネット（商標）等のＬＡＮを構成している。

【００３９】

なお、受信装置２２や、端末２４$_1$，２４$_2$，・・・は、例えば、コンピュータで構成することができる。

【００４０】

また、ここでは、受信装置２２と、端末２４$_1$，２４$_2$，・・・とは、ケーブル

２５で相互に接続することにより、ＬＡＮを構成させるようにしたが、受信装置２２と、端末24_1，24_2，・・・とは、直接接続するようにすることも可能である。

【００４１】

さらに、受信装置２２は、１台の端末24_iとしてのコンピュータのスロットに装着可能なボードとして構成することが可能である。

【００４２】

また、受信装置２２と回線接続装置２３とは、１台のコンピュータで構成することが可能である。

【００４３】

衛星２を介して、送信システム１から送信されてくる衛星放送波は、アンテナ２１で受信され、その受信信号は、受信装置２２に供給される。受信装置２２は、アンテナ２１からの受信信号に対して、後述するような処理を施し、その結果得られるデータを、所定の端末24_iに供給する。

【００４４】

回線接続装置２３は、回線接続装置１５と同様に構成され、ネットワーク４を介しての通信制御を行うようになっている。

【００４５】

端末24_1，24_2，・・・は、例えば、コンピュータで構成され、受信装置２２から必要なデータを受信して、表示、出力、あるいは記憶等するようになっている。

【００４６】

次に、図２のフローチャートを参照して、送信システム１が行うデータの送信処理について説明する。

【００４７】

まず最初に、ステップＳ１において、制御装置１１は、端末24_iに対して送信すべきデータがあるかどうかを判定する。

【００４８】

ここで、制御装置１１は、データを送信するスケジュールが記述されたスケジ

ユール表を有しており、そのスケジュール表に基づいて、端末２４$_i$に対して送信すべきデータがあるかどうかを判定する。また、端末２４$_i$は、回線接続装置２３を制御することにより、ネットワーク４を介して、送信システム１に対して、データを要求することができるようになっており、制御装置１１は、そのような要求が、ネットワーク４を介して回線接続装置１５で受信されたかどうかによって、端末２４$_i$に対して送信すべきデータがあるかどうかを判定する。

【００４９】

ステップＳ１において、端末２４$_1$に対して送信すべきデータがないと判定された場合、ステップＳ２に進み、制御装置１１は、期間を変更するかどうかを判定する。

【００５０】

ここで、送信システム１においては、暗号鍵テーブル記憶部１３における暗号鍵テーブルに記述された暗号鍵が、定期的または不定期に更新されるようになっており、例えば、偶数回目の更新によって得られた暗号鍵を用いて暗号化が行われる期間が、Even期間と呼ばれ、奇数回目の更新によって得られた暗号化器を用いて暗号化が行われる期間が、Odd期間と呼ばれる。従って、Even期間とOdd期間とは交互に現れるが、ステップＳ２では、Even期間からOdd期間に、またはOdd期間からEven期間に変更する時期であるかどうかが判定される。

【００５１】

ステップＳ２において、期間を変更しないと判定された場合、即ち、いま暗号化に用いている暗号鍵をそのまま用いて、データの暗号化を続行する場合、ステップＳ１に戻り、以下、上述の場合と同様の処理を繰り返す。

【００５２】

また、ステップＳ２において、期間を変更すると判定された場合、即ち、いまが、Even期間であるときにはOdd期間に、Odd期間であるときにはEven期間に、期間を変更する場合、ステップＳ３に進み、制御装置１１は、暗号鍵テーブルに記憶された暗号鍵を、後述するステップＳ４において前回生成された暗号鍵に更新し、これにより、その後は、送信処理装置１３において、その更新された暗号鍵を用いて暗号化が行われる。

【００５３】

そして、ステップＳ４に進み、制御装置１１は、次の期間に用いる暗号鍵を生成し（あるいは取得し）、送信処理装置１３に供給して、復号鍵として送信させ、ステップＳ１に戻り、以下、上述の場合と同様の処理が繰り返される。なお、復号鍵の送信は、衛星２を介して行う他、ネットワーク４を介して行うことも可能である。

【００５４】

即ち、次の期間に用いる新たな復号鍵を、その、次の期間の開始直前に、受信システム３に送信したのでは、受信システム３において、新たな復号鍵の設定が、次の期間の開始までに間に合わないことがある。そこで、本実施の形態では、次の期間に用いる新たな暗号鍵は、その直前の期間において、受信システム３に対して配信されるようになっている。

【００５５】

一方、ステップＳ１において、端末24_iに対して送信すべきデータがあると判定された場合、制御装置１１は、データサーバ１２または回線接続装置１５を制御することにより、その送信すべきデータを、送信処理装置１３に供給させる。送信処理装置１３は、データサーバ１２または回線接続装置１５から供給されるデータを受信し、ＩＰパケットにパケット化して、ステップＳ５に進む。

【００５６】

送信処理装置１３は、ステップＳ５において、ＩＰパケットが、暗号化の必要なものであるかどうかを判定し、暗号化の必要なものでないと判定した場合、ステップＳ６およびＳ７をスキップして、ステップＳ８に進む。

【００５７】

また、ステップＳ５において、ＩＰパケットが、暗号化の必要なものであると判定された場合、ステップＳ６に進み、送信処理装置１３は、そのＩＰパケットの宛先となる端末24_iのＭＡＣアドレスに割り当てられた暗号鍵を、暗号鍵テーブルから読み出し、ステップＳ７に進む。ステップＳ７では、送信処理装置１３は、ＩＰパケットを、ステップＳ６で読み出した暗号鍵で暗号化し、ステップＳ８に進む。

【００５８】

ステップＳ８では、送信処理装置は、ＩＰパケットについてＣＲＣ（Cyclic Redundancy Checking)コード（あるいは、チェックサム）を演算し、そのＩＰパケットをペイロードとして、その最後に、ＣＲＣコードを配置するとともに、その先頭に、セクションヘッダを配置することで、図３（Ａ）に示すようなセクションを構成する。なお、ペイロードとＣＲＣコードとの間には、必要に応じて、スタッフィングバイトが挿入される。

【００５９】

セクションヘッダは、図３（Ｂ）に示すように、３バイト（９６ビット）で構成される。ここで、セクションヘッダの詳細については、上述のEN 301 192 V1.1.1(1997-12)に記載されているため、その説明は省略するが、図３（Ｂ）におけるMAC address 1乃至6に、宛先となる４８ビットのＭＡＣアドレスが配置される。ここで、MAC address 1には、ＭＡＣアドレスの最上位ビットから８ビットが配置され、MAC address 2には、その次の上位８ビットが配置される。そして、MAC address 3乃至5それぞれに、同様にしてＭＡＣアドレスが８ビットずつ配置され、MAC address 6には、ＭＡＣアドレスの最下位の８ビットが配置される。

【００６０】

送信処理装置１３は、セクションを構成した後、そのセクションを、所定長のペイロードに分割し、各ペイロードに、ＭＰＥＧ２のトランスポートストリームを構成するＴＳパケットのヘッダを付加することで、ＴＳパケットに類するパケットを構成するカプセル化を行う。そして、送信処理装置１３は、ステップＳ９に進み、その結果得られるパケット（このパケットは、基本的には、ＴＳパケットと同様に処理することができるので、以下、適宜、ＴＳパケットという）に対して、変調、増幅等の必要な処理を施して、アンテナ１４から、衛星放送波として送出し、ステップＳ１に戻る。

【００６１】

なお、図３（Ｂ）に示したセクションヘッダにおいて、その先頭から４３ビット目と４４ビット目の２ビットに配置される２ビットのＰＳＣ(payload_scrambling_control)は、例えば、セクションのペイロードに配置されたデータが暗号化

されているかどうかを表す暗号化判定フラグ、およびそのデータが、Even期間またはOdd期間のうちのいずれの期間のものかを表す期間判定フラグとして用いられるようになっている。

【００６２】

具体的には、例えば、ＰＳＣの下位ビットは、暗号化判定フラグとして用いられ、データが暗号化されているときには１に、暗号化されていないときには０とされる。また、ＰＳＣの上位ビットは、期間判定フラグとして用いられ、Even期間では０に、Odd期間では１にされる。但し、ＰＳＣの上位ビットを、暗号化判定フラグとして用いるとともに、その下位ビットを、期間判定フラグとして用いることも可能である。また、暗号化判定フラグの０と１の割り当てや、期間判定フラグの０と１の割り当ては、上述した場合と逆にすることも可能である。

【００６３】

ここで、ＤＶＢの規格であるEN 301 192 V1.1.1(1997-12)では、ＰＳＣが、００Ｂ（Ｂは、その前に配置された値が２進数であることを表す）の場合が、データが暗号化されていないことを表すこととなっており、従って、暗号化判定フラグは、データが暗号化されているときには１に、暗号化されていないときには０とする方が、ＤＶＢの規格に反しないこととなるので望ましい。

【００６４】

以上のように、図１の放送システムでは、各端末24_iに固有のＭＡＣアドレスに割り当てられた暗号鍵で、データが暗号化されるので、各端末24_iごとの受信制御という、いわば究極の限定受信機構を実現することができる。

【００６５】

なお、ＭＡＣアドレス、あるいはＩＰアドレス等の受信側に固有の値に暗号鍵を割り当てて、きめ細かい受信制御を行う限定受信機構を実現する方法については、本件出願人が先に提案した、例えば、特開平１０－２１５２４４号公報に、その詳細が開示されている。但し、わが国における通信衛星放送が、ＤＶＢ－ＳＩ(Digtal Video Broadcasting - Service Information / EN300 468)から派生した仕様に準拠している現状においては、上述したように、ＭＡＣアドレスを用いるのが、その仕様に適合することとなる。

【００６６】

次に、図４は、図１の受信装置２２の構成例を示している。

【００６７】

アンテナ２１は、衛星２を介して、送信システム１から送信されてくる衛星放送波を受信し、その受信信号を、フロントエンド部３１に出力する。フロントエンド部３１は、ＣＰＵ３４の制御にしたがい、アンテナ２１からの受信信号から所定のチャンネルの信号を選局し、さらに、その信号を、ＴＳパケットのディジタルストリーム(IP_datagram_data_byte)に復調して、デマルチプレクサ３２に出力する。デマルチプレクサ３２は、ＣＰＵ３４の制御にしたがい、フロントエンド部３１からのディジタルストリームから、所定のＴＳパケットを抽出し、復号ＬＳＩ(Large Scale Integrated Circuit)３３に出力する。即ち、デマルチプレクサ３２は、フロントエンド部３１からのディジタルストリームを構成するＴＳパケットのヘッダに配置されているＰＩＤ(Packet Identification)に基づいて、ＴＳパケットの取捨選択を行い、選択したＴＳパケットのみを、復号ＬＳＩ３３に出力する。

【００６８】

復号ＬＳＩ３３は、１チップのＬＳＩで、フィルタ４１、復号器４２、鍵テーブル記憶部４３、チェッカ４４、およびＦＩＦＯ(First In First Out)バッファ４５で構成されている。

【００６９】

フィルタ４１は、ＣＰＵ３４の制御にしたがい、デマルチプレクサ３２からのＴＳパケットで構成されるセクションのペイロードに配置されたデータを、必要に応じて検査し、不必要なＴＳパケットを破棄し、必要なＴＳパケットだけを復号器４２に出力する。

【００７０】

復号器４２は、フィルタ４１からのＴＳパケットで構成されるセクションのペイロードに配置されたデータ（ここでは、ＩＰパケット）を、鍵テーブル記憶部４３に記憶された復号鍵で復号し、チェッカ４４に出力する。また、復号器４２は、図２で説明したように、送信システム１において暗号鍵が更新され、その更

新された暗号鍵が送信されてきた場合、ＣＰＵ３４の制御にしたがい、その暗号鍵を、復号鍵として、鍵テーブル記憶部４３の記憶内容を更新する。従って、ここでは、暗号化方式として、共通鍵暗号化方式が用いられるようになっている。但し、暗号化方式としては、公開鍵暗号化方式を用いることも可能である。

【００７１】

鍵テーブル記憶部４３は、受信装置２２にケーブル２５を介して接続された端末24_1，24_2，・・・それぞれのＭＡＣアドレスと、それぞれに割り当てられた復号鍵とが対応付けられて登録された鍵テーブルを記憶している。

【００７２】

チェッカ４４は、ＣＰＵ３４の制御にしたがい、復号器４２が出力するＩＰパケットについて、そのＩＰパケットが配置されていたセクションのＣＲＣコードを用いて誤り検出を行い、これにより、復号器４２における復号が正常に行われたかどうか等を判定する。チェッカ４４で処理されたＩＰパケットは、ＦＩＦＯバッファ４５に供給されるようになっており、ＦＩＦＯバッファ４５は、チェッカ４４からのＩＰパケットを一時記憶し、ＣＰＵ３４の制御にしたがい、記憶したＩＰパケットを、Ｉ／Ｆ(Interface)３５に出力する。これにより、ＩＰパケットのデータレートが調整される。

【００７３】

ＣＰＵ３４は、フロントエンド部３１、デマルチプレクサ３２、復号ＬＳＩ３３、およびＩ／Ｆ３５を制御する。Ｉ／Ｆ３５は、ＣＰＵ３４の制御にしたがい、ＦＩＦＯバッファ４５からのＩＰパケットを、ケーブル２５を介して、端末24_iに供給するインタフェースとして機能する。

【００７４】

次に、図５は、図４の鍵テーブル記憶部４３に記憶されている鍵テーブルの構成例を示している。

【００７５】

鍵テーブルは、例えば、ケーブル２５に接続されている端末24_1，24_2，・・・の数と同一数のエントリから構成されている。図５では、鍵テーブルは、Ｎ個のエントリ＃１乃至＃Ｎを有しており、従って、本実施の形態では、ケーブル

２５には、Ｎ個の端末２４_{1}乃至２４_{N}が接続されている。なお、鍵テーブルのエントリの最大数は、鍵テーブル記憶部４３の記憶容量等によって制限される。

【００７６】

各エントリ＃ｉ（Ｉ＝１，２，・・・，Ｎ）には、端末２４_{i}の４８ビットのＭＡＣアドレスMACaddress#iと、そのＭＡＣアドレスに割り当てられたｍビットの復号鍵（ｍは、使用する暗号形式による）とが対応付けられて登録されている。なお、本実施の形態では、上述したように、Even期間とOdd期間とが存在し、それぞれの期間では、異なる暗号鍵で暗号化が行われるため、各エントリ＃ｉには、Even期間に暗号化されたデータを復号するための復号鍵（以下、適宜、Even復号鍵という）$K_{Even\#i}$と、Odd期間に暗号化されたデータを復号するための復号鍵（以下、適宜、Odd復号鍵という）$K_{Odd\#i}$との２つの復号鍵が登録されている。

【００７７】

さらに、各エントリ＃ｉのＭＡＣアドレスMACaddress#iの先頭には、そのエントリ＃ｉが有効であるかどうかを表すValidビット（以下、適宜、エントリValidビットという）が付加されている。また、各エントリ＃ｉのEven復号鍵$K_{Even\#i}$とOdd復号鍵$K_{Odd\#i}$にも、それぞれが有効かどうかを表すValidビット（以下、適宜、復号鍵Validビットという）が付加されている。

【００７８】

ここで、エントリValidビット、復号鍵Validビットは、例えば、それが１の場合が有効であることを表し、０の場合が有効でないことを表す。但し、エントリValidビット、復号鍵Validビットの０と１の割り当ては、上述した場合と逆にすることも可能である。

【００７９】

上述したように、送信システム１においては、次の期間に用いる新たな暗号鍵と同一の復号鍵は、その直前の期間に、受信システム３に対して配信されるようになっている。従って、Even期間においては、その次のOdd期間で用いられる暗号鍵と同一の復号鍵（Odd復号鍵）が配信され、Odd期間においては、その次のEven期間で用いられる暗号鍵と同一の復号鍵（Even復号鍵）が配信される。そして

、復号器４２では、ＣＰＵ３４の制御の下、そのようにして配信されてくる復号鍵が、鍵テーブルに設定（例えば、上書き）される。従って、この場合、鍵テーブルには、次の期間に用いられる復号鍵が、現在の期間が終了するまでに設定され、さらに、期間の変更に伴う復号鍵の変更は、ＣＰＵ３４を介在せずに、復号器４２が読み出しを行う鍵テーブルの位置（アドレス）を切り替えるだけで済むので、瞬時に行うことができる。

【００８０】

次に、図６のフローチャートを参照して、図４の受信装置２２の動作について説明する。

【００８１】

アンテナ２１では、衛星２を介して、送信システム１から送信されてくる衛星放送波が受信され、その結果得られる受信信号は、フロントエンド部３１およびデマルチプレクサ３２を介することにより、ＴＳパケットのディジタルストリームとされ、復号ＬＳＩ３３に供給される。

【００８２】

復号ＬＳＩ３３では、デマルチプレクサ３２が出力するＴＳパケットで構成されるセクションが、フィルタ４１を介して、復号器４２に供給される。復号器４２は、セクションを受信し、ステップＳ１１において、そのセクションヘッダに配置されたＭＡＣアドレスを、内蔵するレジスタとしての変数ＭＡにセットする。

【００８３】

復号器４２は、鍵テーブルを参照することにより、変数ＭＡに一致するＭＡＣアドレスのエントリを検索し、即ち、鍵テーブルのエントリ＃１から順に、各エントリ＃ｉに登録されているＭＡＣアドレスを読み出して、そのＭＡＣアドレスと、変数ＭＡとを比較（照合）し、ステップＳ１２において、変数ＭＡに一致するＭＡＣアドレスのエントリが存在するかどうかを判定する。ステップＳ１２において、変数ＭＡに一致するＭＡＣアドレスのエントリが存在しないと判定された場合、即ち、セクションヘッダに配置されたＭＡＣアドレスを有する端末が、ケーブル２５上に接続されていない場合、ステップＳ１３に進み、復号器４２は

、そこに供給されたセクションを破棄し、処理を終了する。

【００８４】

また、ステップＳ１２において、変数ＭＡに一致するＭＡＣアドレスのエントリが存在すると判定された場合、そのエントリを注目エントリとして、ステップＳ１４に進む。

【００８５】

ステップＳ１４では、復号器４２は、注目エントリのエントリValidビットに基づいて、その注目エントリが有効であるかどうかを判定する。ステップＳ１４において、注目エントリが有効でないと判定された場合、即ち、注目エントリのエントリValidビットが０である場合、ステップＳ１３に進み、復号器４２は、そこに供給されたセクションを破棄し、処理を終了する。

【００８６】

従って、復号器４２に供給されたセクションのセクションヘッダに配置されたＭＡＣアドレスを有する端末が、ケーブル２５上に接続されている場合でも、そのＭＡＣアドレスのエントリが有効とされていないときには、そのセクションは、ケーブル２５上の端末に供給されない。

【００８７】

また、ステップＳ１４において、注目エントリが有効であると判定された場合、即ち、注目エントリのエントリValidビットが１である場合、ステップＳ１５に進み、復号器４２は、セクションヘッダのＰＳＣ（図３（Ｂ））の下位ビット、即ち、暗号化判定フラグを参照し、セクションのペイロードのデータ（ＩＰパケット）が暗号化されているかどうかを判定する。ステップＳ１５において、暗号化判定フラグが０であると判定された場合、即ち、セクションのペイロードに配置されたＩＰパケットが暗号化されていない場合、ステップＳ１７およびＳ１８をスキップして、ステップＳ１９に進み、復号器４２は、その暗号化されていないＩＰパケットを、チェッカ４４を介して、ＦＩＦＯバッファ４５に出力して、処理を終了する。

【００８８】

そして、ＦＩＦＯバッファ４５に記憶されたＩＰパケットは、Ｉ／Ｆ３５を介

して、そのＩＰパケットが配置されていたセクションのセクションヘッダにおけるＭＡＣアドレスによって特定されるケーブル２５上の端末24_iに供給される。

【００８９】

一方、ステップＳ１５において、暗号化判定フラグが１であると判定された場合、即ち、セクションのペイロードに配置されたＩＰパケットが暗号化されている場合、ステップＳ１６に進み、復号器４２は、そのセクションのセクションヘッダのＰＳＣ（図３（Ｂ））の上位ビット、即ち、期間判定フラグを、内蔵するレジスタとしての変数ＥＯにセットして、ステップＳ１７に進む。

【００９０】

ステップＳ１７では、復号器４２は、ＭＡＣアドレスが変数ＭＡに一致する注目エントリにおける変数ＥＯに対応する期間、即ち、変数ＥＯが０である場合にはEven期間、１である場合にはOdd期間の復号鍵の復号鍵Validビット＃（ＭＡ，ＥＯ）が有効であるかどうかを判定する。ステップＳ１７において、復号鍵Validビット＃（ＭＡ，ＥＯ）が有効でないと判定された場合、即ち、復号鍵Validビット＃（ＭＡ，ＥＯ）が０である場合、ステップＳ１３に進み、復号器４２は、そこに供給されたセクションを破棄し、処理を終了する。

【００９１】

従って、復号器４２に供給されたセクションのセクションヘッダに配置されたＭＡＣアドレスを有する端末が、ケーブル２５上に接続されており、そのＭＡＣアドレスのエントリが有効とされている場合でも、期間判定フラグが表す期間の復号鍵が有効とされていないときには、そのセクションは、ケーブル２５上の端末に供給されない。

【００９２】

一方、ステップＳ１７において、復号鍵Vaildフラグ＃（ＭＡ，ＥＯ）が有効であると判定された場合、即ち、復号鍵Validビット＃（ＭＡ，ＥＯ）が１である場合、ステップＳ１８に進み、復号器４２は、ＭＡＣアドレスが変数ＭＡに一致する注目エントリにおける、変数ＥＯに対応する期間の復号鍵Ｋｅｙ（ＭＡ，ＥＯ）を、鍵テーブルから読み出し、その復号鍵Ｋｅｙ（ＭＡ，ＥＯ）で、セク

ションのペイロードに配置されたＩＰパケットを復号し、ステップＳ１９に進む。

【００９３】

ステップＳ１９では、復号器４２は、復号されたＩＰパケットを、チェッカ４４を介して、ＦＩＦＯバッファ４５に出力して、処理を終了する。

【００９４】

そして、ＦＩＦＯバッファ４５に記憶されたＩＰパケットは、Ｉ／Ｆ３５を介して、そのＩＰパケットが配置されていたセクションのセクションヘッダにおけるＭＡＣアドレスによって特定されるケーブル２５上の端末24_iに供給される。

【００９５】

なお、図６のフローチャートにしたがった処理は、復号器４２に対して、セクションが供給されるごとに行われる。

【００９６】

以上のように、鍵テーブルのエントリに登録されたエントリValidビットに基づいて、そのエントリが有効かどうかを判定し、端末に対するデータの出力を制御するようにしたので、データを正常に取得する（受信する）ことのできるユーザ（端末）を、容易に制限することが可能となる。

【００９７】

さらに、鍵テーブルの復号鍵Validビットにも基づいて、データの出力を制御するようにしたので、例えば、ある端末について、Even期間またはOdd期間のうちのいずれか一方の期間のみのデータの受信を許可し、他方の期間のデータの受信を禁止することを、容易に行うことができる。

【００９８】

なお、エントリValidビットおよび復号鍵Validビットの設定は、受信装置２２において、いわば自主的に行うことも可能であるし、また、送信システム１から送信されてくる情報に基づいて行うことも可能である。

【００９９】

また、本実施の形態では、復号鍵を（暗号鍵も）、端末に固有のＭＡＣアドレ

スに割り当てるようにしたが、復号鍵は、その他、例えば、端末に固有の端末ＩＤ(Identification)を設定し、その端末ＩＤに割り当てるようにすることも可能である。さらに、復号鍵は、複数の端末ごとに固有のグループＩＤを設定し、そのグループＩＤごとに割り当てるようにすることも可能である。但し、ＭＡＣアドレスに対して復号鍵を割り当てる場合には、上述したようなきめの細かい限定受信機構を、ＤＶＢの規格であるEN 301 192 V1.1.1(1997-12)に準拠したディジタル衛星放送の枠組みに、容易に組み込むことが可能となる。

【０１００】

また、本実施の形態では、フィルタ４１、復号器４２、鍵テーブル記憶部４３、チェッカ４４、およびＦＩＦＯバッファ４５を、１チップの復号ＬＳＩ３３で構成するようにしたが、フィルタ４１、復号器４２、鍵テーブル記憶部４３、チェッカ４４、およびＦＩＦＯバッファ４５は、それぞれ別のチップとして構成することも可能である。但し、フィルタ４１、復号器４２、鍵テーブル記憶部４３、チェッカ４４、およびＦＩＦＯバッファ４５を、１チップの復号ＬＳＩ３３で構成した方が、データの復号が、復号ＬＳＩ３３の外部から完全に隠蔽された形で行われるため、セキュリティを向上させることができる。さらに、回路の実装面積の縮小や、処理の高速化等の観点からも、フィルタ４１、復号器４２、鍵テーブル記憶部４３、チェッカ４４、およびＦＩＦＯバッファ４５は、１チップの復号ＬＳＩ３３で構成するのが望ましい。

【０１０１】

また、本実施の形態では、ディジタル衛星放送によってデータを配信する場合について説明したが、本発明は、その他、例えば、マルチキャストでデータを配信する場合等にも適用可能である。

【０１０２】

さらに、本実施の形態では、Even期間とOdd期間の２つの期間を設けるようにしたが、そのような期間を設けないようにすることも可能であるし、３以上の期間を設けるようにすることも可能である。同様に、鍵テーブルの各エントリに登録する復号鍵の数も、１つだけとしたり、３以上とすることが可能である。

【０１０３】

また、本実施の形態では、データを、ＤＶＢの規格に準拠する形で配信するようにしたが、データの配信は、ＤＶＢの規格に準拠しない形で行うことも可能である。

【０１０４】

次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや、１チップのマイクロコンピュータ等にインストールされる。

【０１０５】

そこで、図７は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【０１０６】

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク１０５やＲＯＭ１０３に予め記録しておくことができる。

【０１０７】

あるいはまた、プログラムは、フロッピーディスク、CD-ROM(Compact Disc Read Only Memory), MO(Magneto optical)ディスク, DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体１１１に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体１１１は、いわゆるパッケージソフトウエアとして提供することができる。

【０１０８】

なお、プログラムは、上述したようなリムーバブル記録媒体１１１からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部１０８で受信し、内蔵するハードディスク１０５にインストールすることができる。

【０１０９】

コンピュータは、CPU(Central Processing Unit)１０２を内蔵している。CPU１０２には、バス１０１を介して、入出力インタフェース１１０が接続されており、CPU１０２は、入出力インタフェース１１０を介して、ユーザによって、キーボードやマウス等で構成される入力部１０７が操作されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)１０３に格納されているプログラムを実行する。あるいは、また、CPU１０２は、ハードディスク１０５に格納されているプログラム、衛星若しくはネットワークから転送され、通信部１０８で受信されてハードディスク１０５にインストールされたプログラム、またはドライブ１０９に装着されたリムーバブル記録媒体１１１から読み出されてハードディスク１０５にインストールされたプログラムを、RAM(Random Access Memory)１０４にロードして実行する。これにより、CPU１０２は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU１０２は、その処理結果を、必要に応じて、例えば、入出力インタフェース１１０を介して、LCD(Liquid CryStal Display)やスピーカ等で構成される出力部１０６から出力、あるいは、通信部１０８から送信、さらには、ハードディスク１０５に記録等させる。

【０１１０】

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【０１１１】

また、プログラムは、１のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【０１１２】

【発明の効果】

本発明のデータ処理装置およびデータ処理方法、並びに記録媒体によれば、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照することで、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリが、注目エントリとして検索される。そして、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかが判定され、その判定結果に基づいて、データブロックに配置されたデータの出力が制御される。従って、データを正常に取得することのできるユーザを、容易に制限することが可能となる。

【図面の簡単な説明】

【図１】

本発明を適用した放送システムの一実施の形態の構成例を示すブロック図である。

【図２】

図１の送信システム１の処理を説明するためのフローチャートである。

【図３】

セクションとセクションヘッダのフォーマットを示す図である。

【図４】

図１の受信装置２２の構成例を示すブロック図である。

【図５】

鍵テーブルを示す図である。

【図６】

図４の受信装置２２の処理を説明するためのフローチャートである。

【図７】

本発明を適用したコンピュータの一実施の形態の構成例を示すブロック図である。

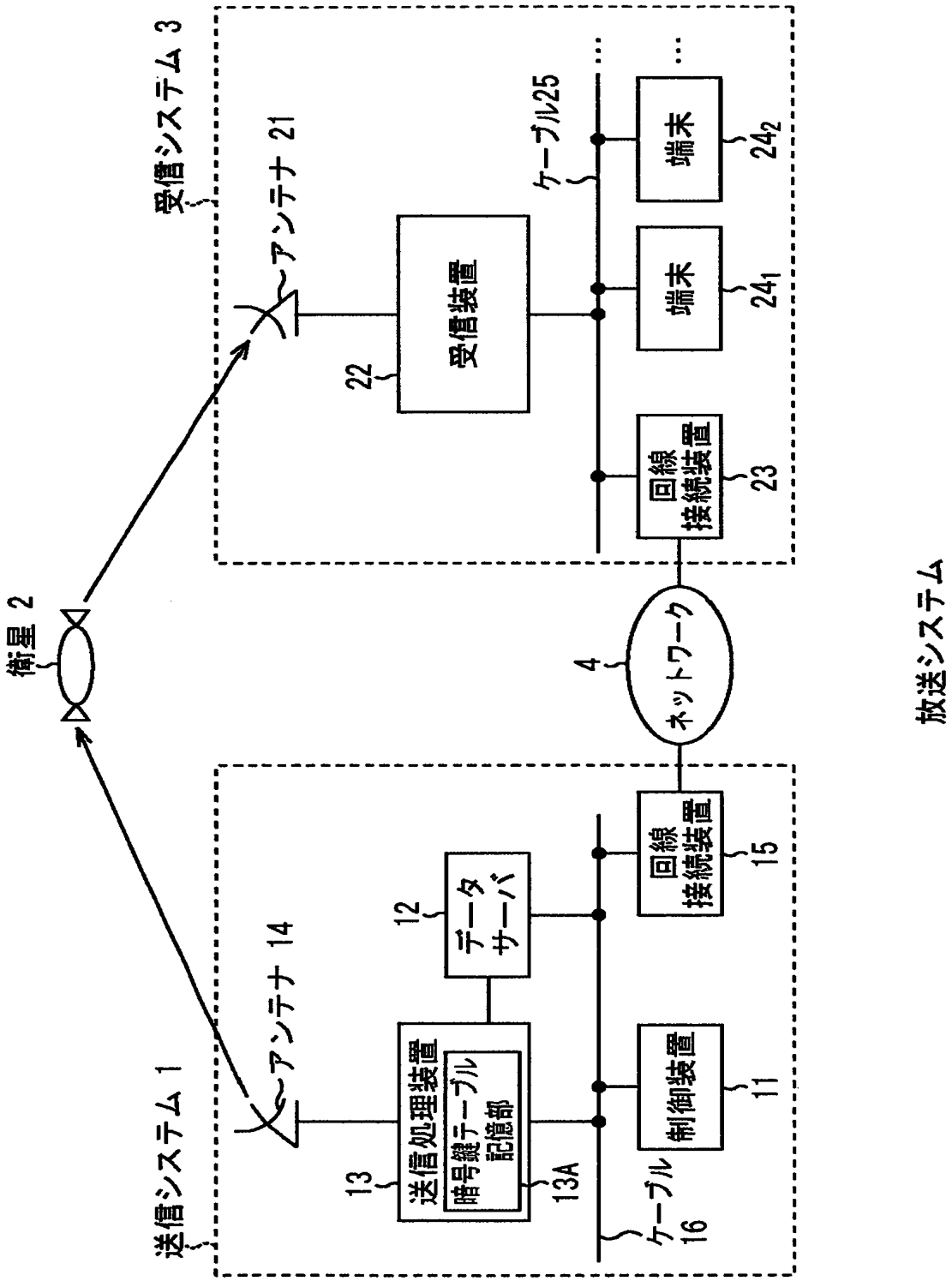
【符号の説明】

１　送信システム，　２　衛星，　３　受信システム，　４　ネットワーク，　１１　制御装置，　１２　データサーバ，　１３　送信処理装置，　１３Ａ　暗号鍵テーブル記憶部，　１４　アンテナ，　１５　回線接続装置，　１６　ケ

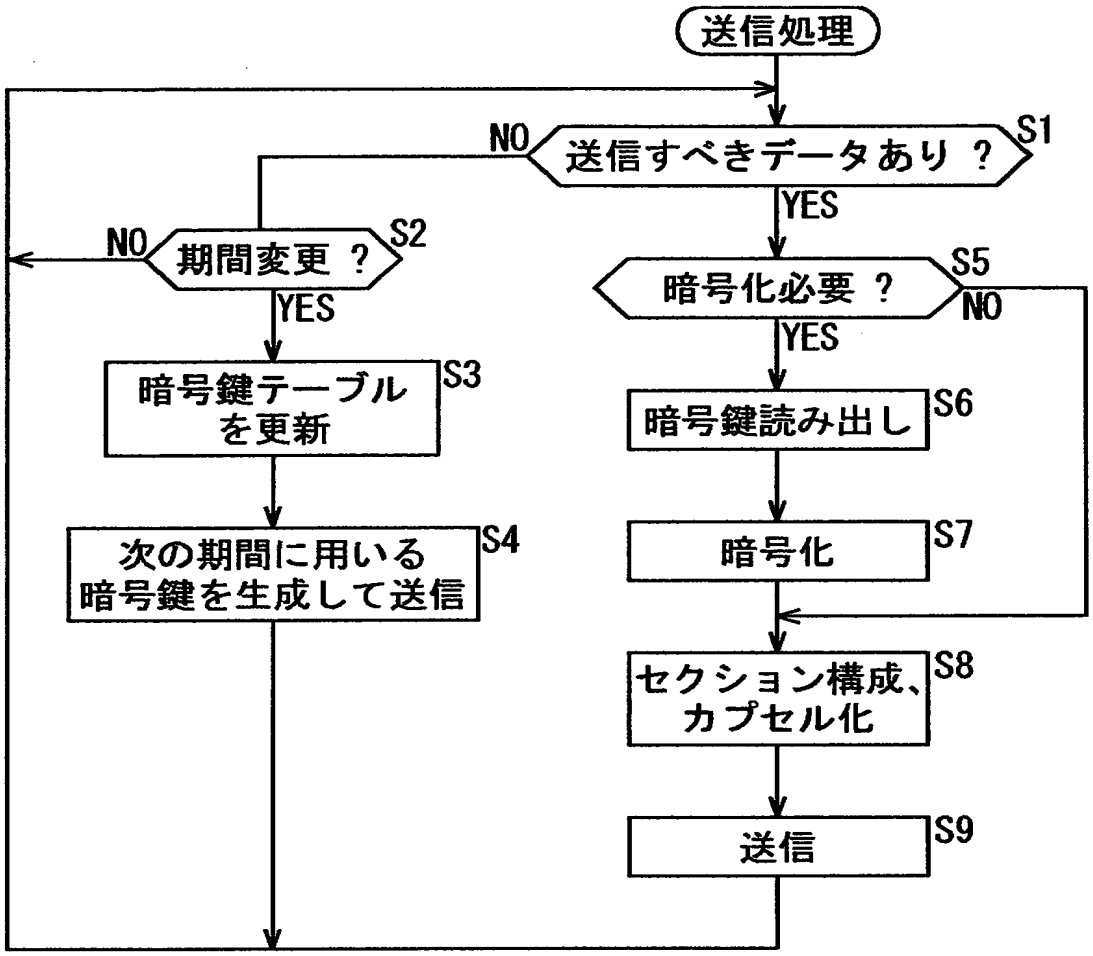
ーブル，　２１　アンテナ，　２２　受信装置，　２３　回線接続装置，　２４$_1$，２４$_2$　端末，　３１　フロントエンド部，　３２　デマルチプレクサ，　３３　復号ＬＳＩ，　３４　ＣＰＵ，　３５　Ｉ／Ｆ，　４１　フィルタ，　４２　復号器，　４３　鍵テーブル記憶部，　４４　チェッカ，　４５　ＦＩＦＯバッファ，　１０１　バス，　１０２　CPU，　１０３　ROM，　１０４　RAM，　１０５　ハードディスク，　１０６　出力部，　１０７　入力部，　１０８　通信部，　１０９　ドライブ，　１１０　入出力インタフェース，　１１１　リムーバブル記録媒体

【書類名】図面

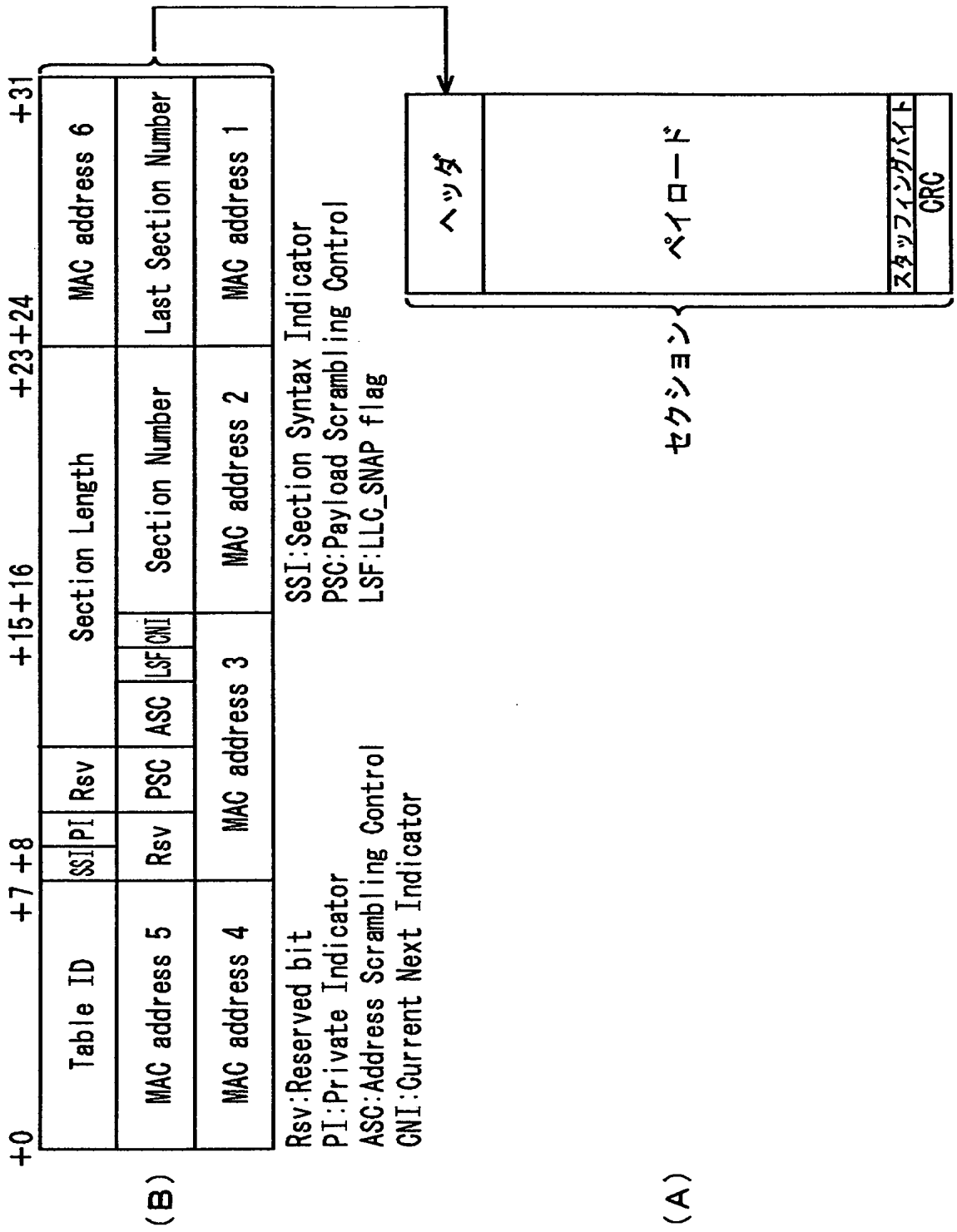
【図１】


送信システム 1
受信システム 3
衛星 2
アンテナ 14
アンテナ 21
送信処理装置
暗号鍵テーブル記憶部
13
13A
データサーバ
12
受信装置
22
回線接続装置
15
回線接続装置
23
制御装置
11
ケーブル16
ケーブル25
端末
24₁
端末
24₂
ネットワーク
4
放送システム

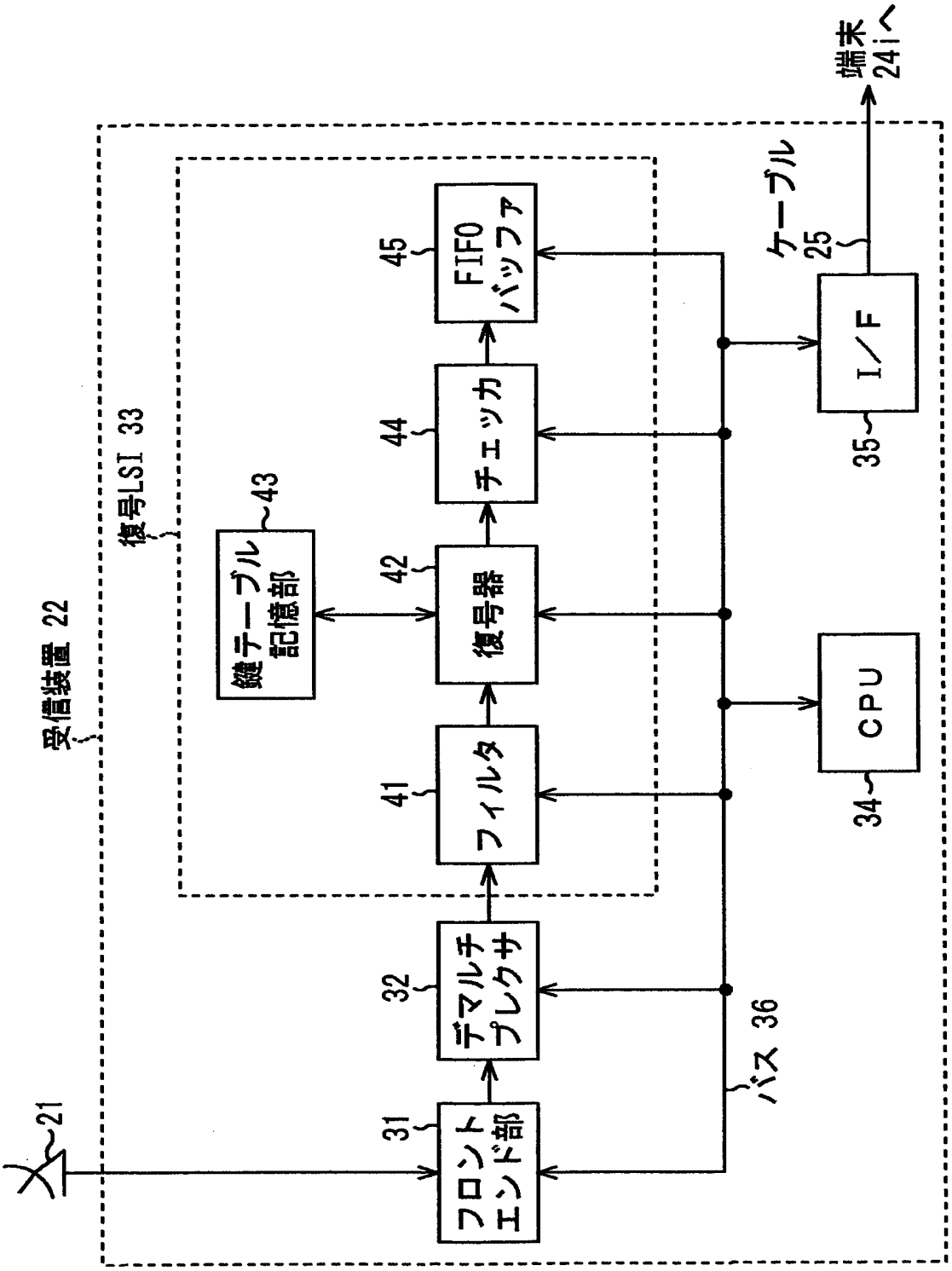
【図２】


送信処理
送信すべきデータあり ？
S1
NO
YES
期間変更 ？
S2
NO
YES
暗号鍵テーブル
を更新
S3
次の期間に用いる
暗号鍵を生成して送信
S4
暗号化必要 ？
S5
NO
YES
暗号鍵読み出し
S6
暗号化
S7
セクション構成、
カプセル化
S8
送信
S9

【図３】


(A)
セクション
ヘッダ
ペイロード
スタッフィングバイト
CRC
(B)
+0
+7 +8
+15 +16
+23 +24
+31
Table ID
SSI
PI
Rsv
Section Length
MAC address 6
MAC address 5
Rsv
PSC
ASC
LSF
CNI
Section Number
Last Section Number
MAC address 4
MAC address 3
MAC address 2
MAC address 1
Rsv:Reserved bit
PI:Private Indicator
ASC:Address Scrambling Control
CNI:Current Next Indicator
SSI:Section Syntax Indicator
PSC:Payload Scrambling Control
LSF:LLC_SNAP flag

【図４】

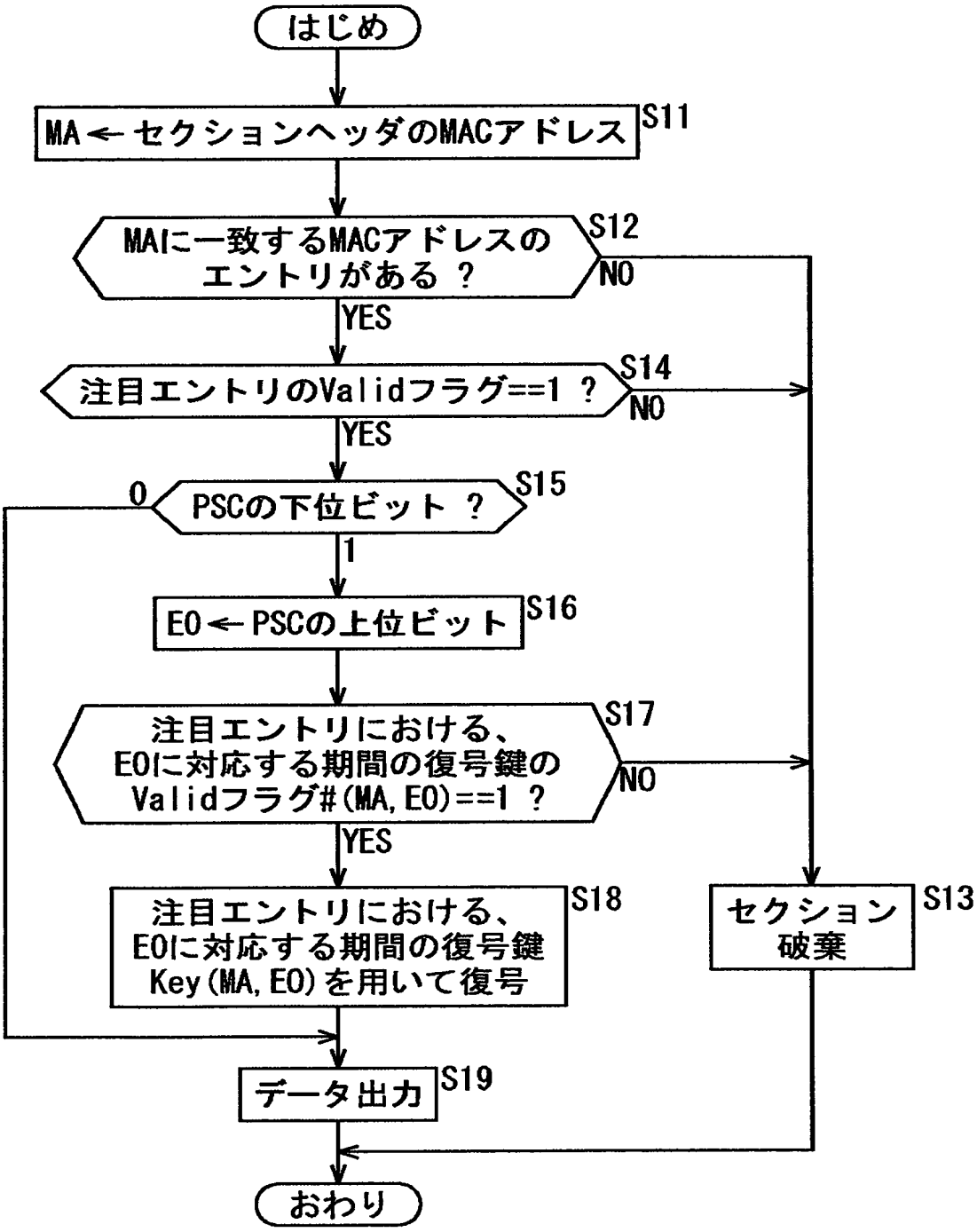

受信装置 22
復号LSI 33
21
フロントエンド部
31
デマルチプレクサ
32
フィルタ
41
復号器
42
チェッカ
44
FIFOバッファ
45
鍵テーブル記憶部
43
バス 36
CPU
34
I／F
35
ケーブル
25
端末
24iへ

【図５】

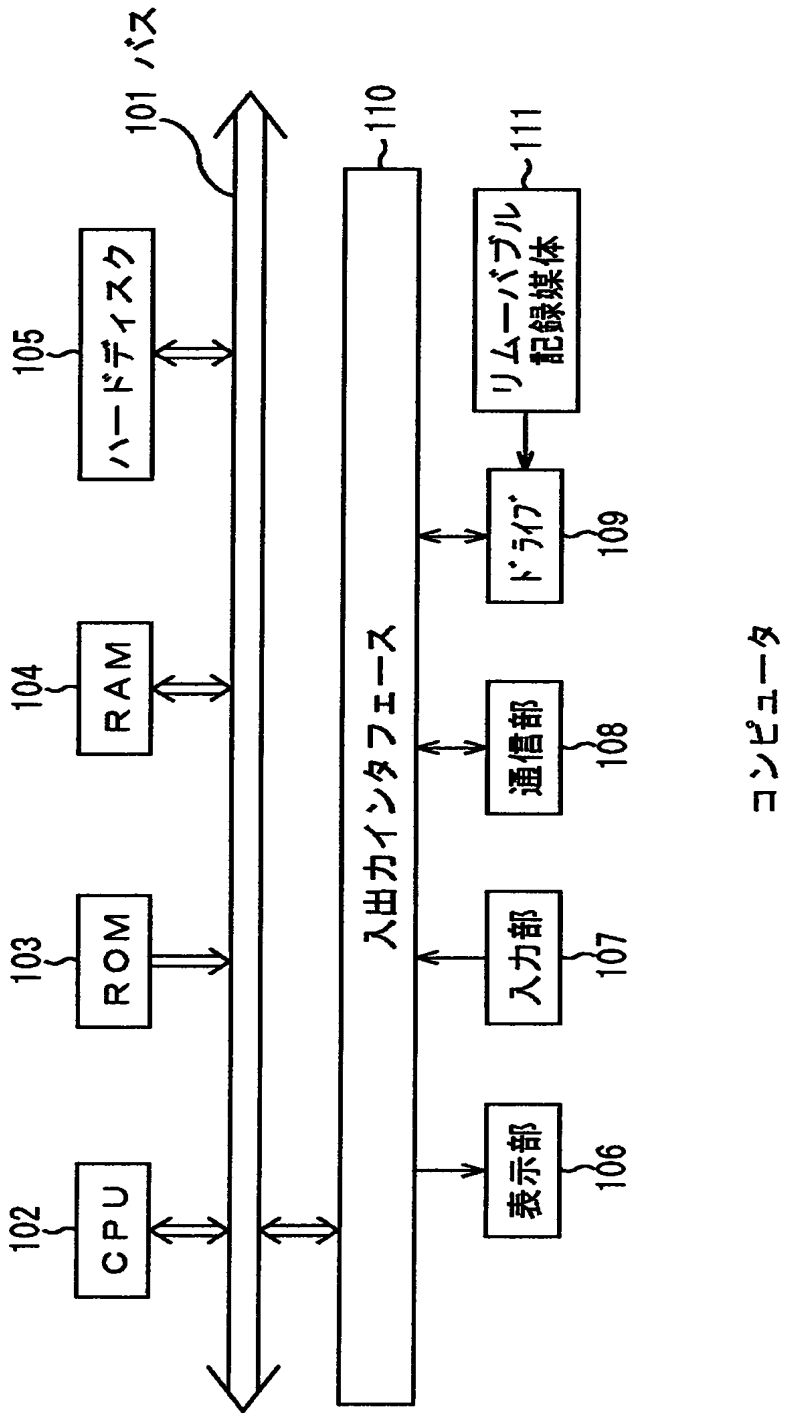

エントリ#1
Valid
MAC address #1(48bit)
Valid
KEven#1(m bit)
Valid
KOdd#1(m bit)
エントリ#2
Valid
MAC address #2(48bit)
Valid
KEven#2(m bit)
Valid
KOdd#2(m bit)
エントリ#3
Valid
MAC address #3(48bit)
Valid
KEven#3(m bit)
Valid
KOdd#3(m bit)
エントリ#N
Valid
MAC address #N(48bit)
Valid
KEven#N(m bit)
Valid
KOdd#N(m bit)

鍵テーブル

【図６】


はじめ
MA←セクションヘッダのMACアドレス
S11
MAに一致するMACアドレスの
エントリがある ？
S12
NO
YES
注目エントリのValidフラグ==1 ？
S14
NO
YES
0
PSCの下位ビット ？
S15
1
E0←PSCの上位ビット
S16
注目エントリにおける、
E0に対応する期間の復号鍵の
Validフラグ#(MA, E0)==1 ？
S17
NO
YES
注目エントリにおける、
E0に対応する期間の復号鍵
Key(MA, E0)を用いて復号
S18
セクション
破棄
S13
データ出力
S19
おわり

【図７】


101 バス
110
111
リムーバブル記録媒体
105
ハードディスク
ドライブ
109
104
RAM
通信部
108
入出力インタフェース
103
ROM
入力部
107
102
CPU
表示部
106
コンピュータ

【書類名】　　要約書

【要約】

【課題】　データを正常に取得することのできるユーザを、容易に制限する。

【解決手段】　鍵テーブルの各エントリ＃ｉには、端末のＭＡＣアドレスMACaddress#iと、そのＭＡＣアドレスに割り当てられている復号鍵$K_{Even\#i}$および$K_{Odd\#i}$とが対応付けられて登録されている。さらに、各エントリ＃ｉのＭＡＣアドレスMACaddress#iには、そのエントリ＃ｉが有効であるかどうかを表すValidビットが付加されている。この場合において、受信されたセクションのセクションヘッダに配置されているのと同一のＭＡＣアドレスが、鍵テーブルから検索され、そのＭＡＣアドレスのエントリが有効かどうかが、Validビットに基づいて判定される。そして、エントリが有効である場合のみ、セクションのペイロードに配置されたデータが復号されて出力される。

【選択図】　　図５

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
　〔変更理由〕　新規登録
　　住　所　　東京都品川区北品川６丁目７番３５号
　　氏　名　　ソニー株式会社